PAUL D. PETERS| DEPUTY ASSISTANT SECRETARY OF DEFENSE
SUPPLY CHAIN INTEGRATION

ANTI-COUNTERFEIT

PRODUCT SUPPORT MANAGERS CONFERENCE

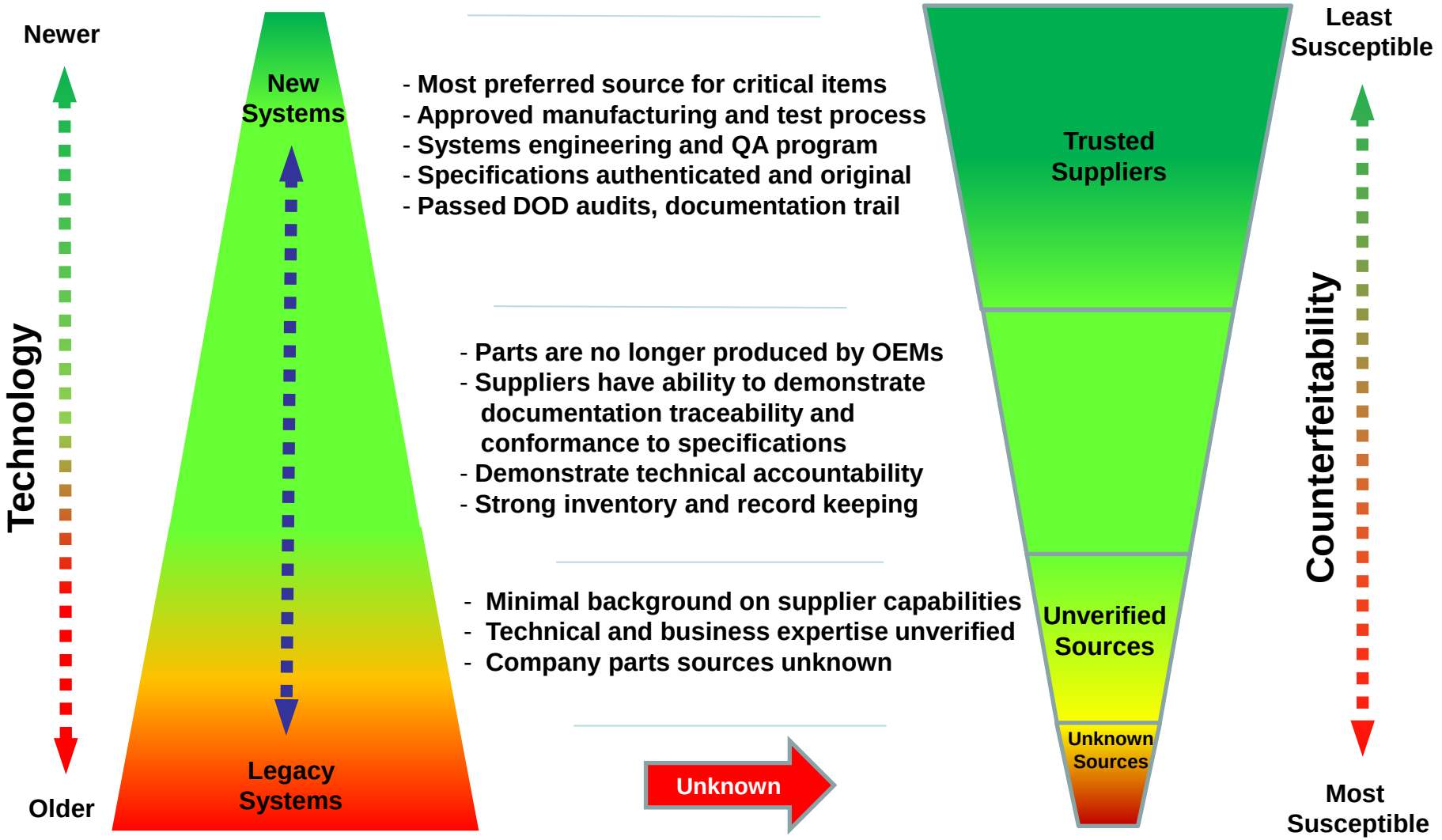
6 JUNE 2012

Areas of Focus

- Counterfeit prevention & detection
  - Risk and supply chain implications
  - Legislation, policy and current activities
- Counterfeit identification and disposition
- Counterfeit reporting and information sharing

Profile of Counterfeit Risk

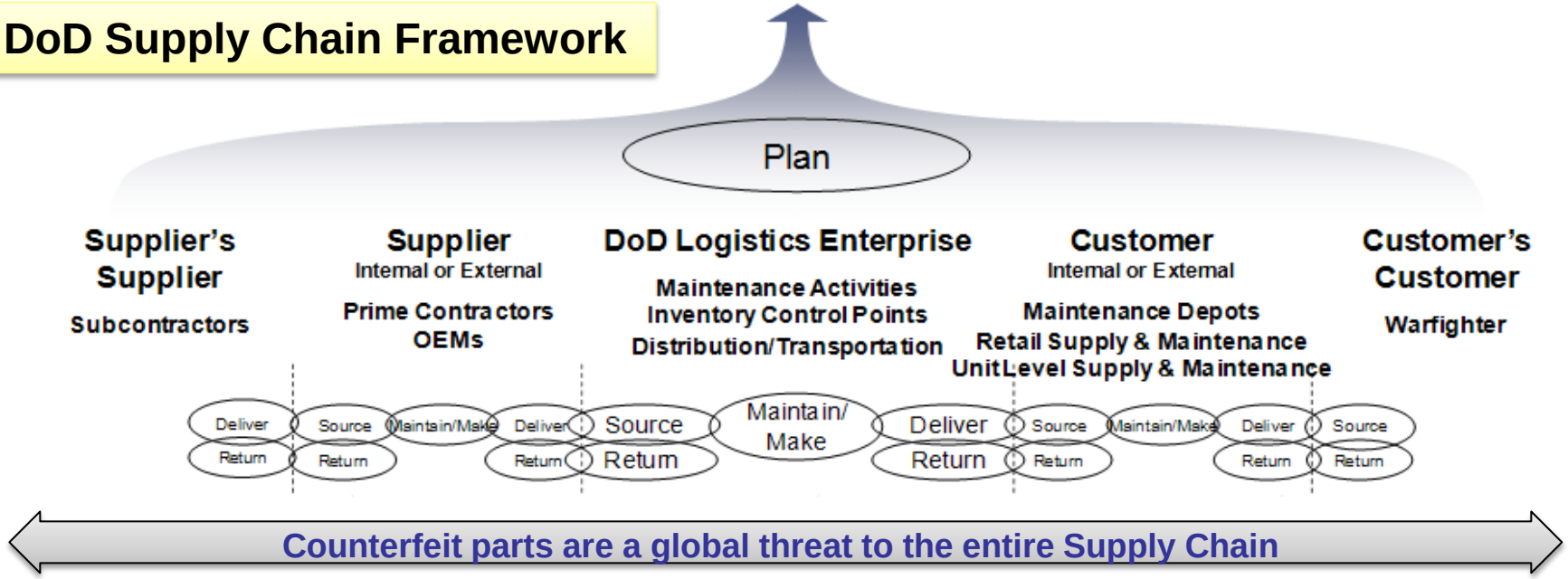
OEM/OCM/
Authorized
Distributors



Prolonged use of aging systems creates opportunities for counterfeit parts to enter the supply chain

Supply Chain Implications

DoD Supply Chain Framework



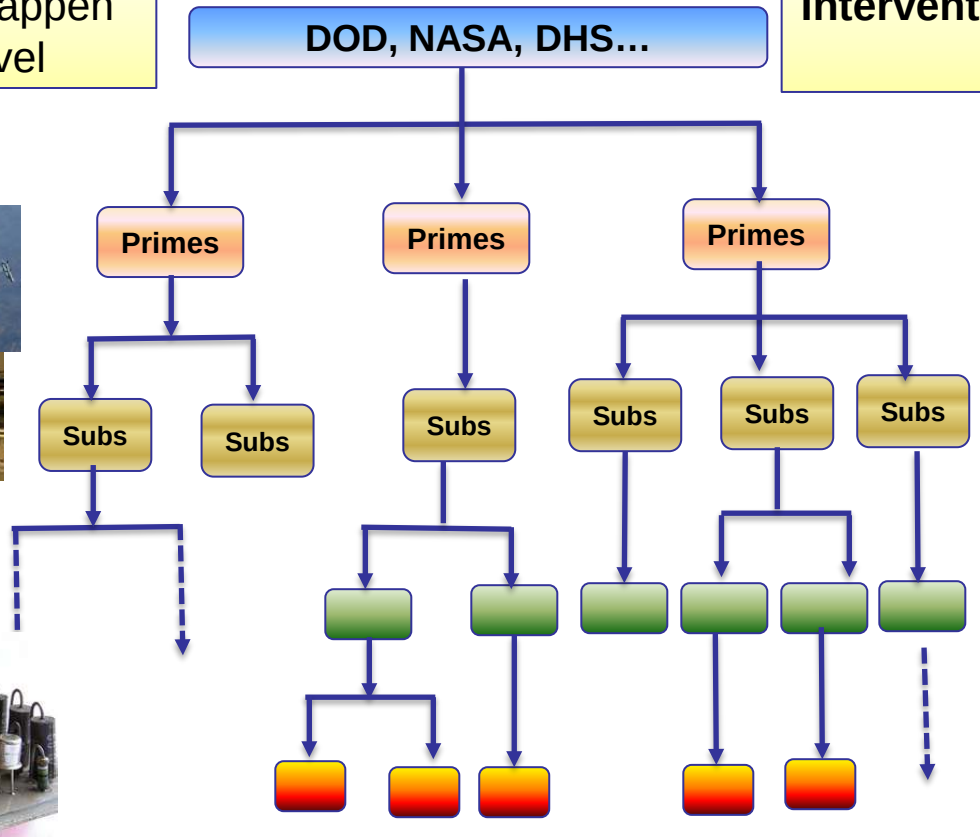
Anti-Counterfeit Touch Points

- Plan: Collaboration with Trusted Suppliers
- Source: Reaches all levels of the supply chain
- Make: Demands genuineness of all critical parts
- Deliver: Standards and practice
- Return: Prevent counterfeit reentry into the supply chain

Intrusion and Intervention

Intrusion…can happen at any level

Intervention…requires more than just contract action



Systems

Titan IV, GPS, F-16 etc.

Sub-Systems

Flight Avionics, Propulsion, Electro-Mechanical Valves, Guidance Computer, INS, etc.

Components

Power Distribution Assembly, Data Recorder, Antenna Assembly, etc.

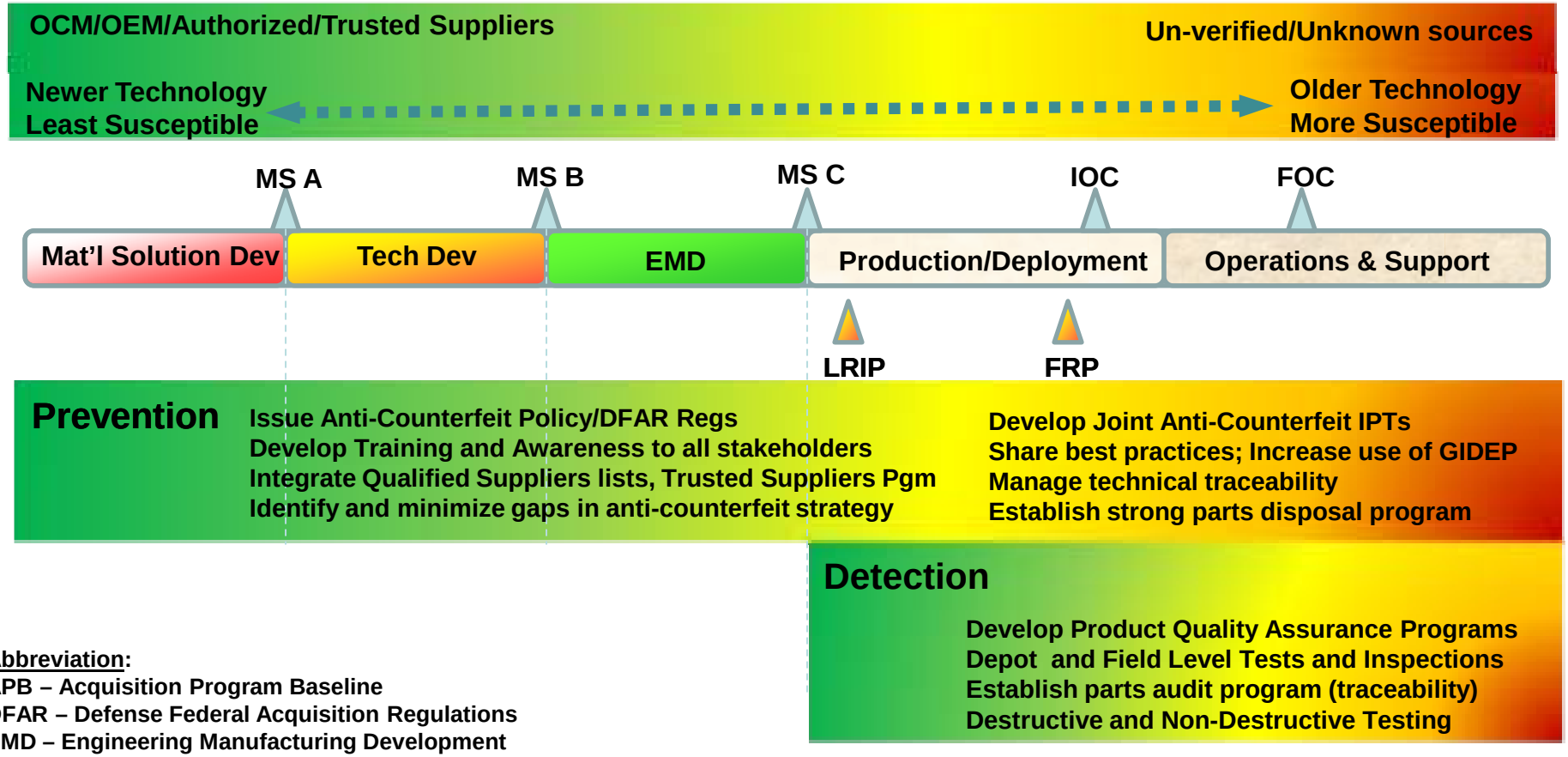
Sub-Components

Graphic Cards, Circuit boards, Micro chips, diodes, capacitors, etc.

Counterfeit Parts Entering Supply Chain

OCM/OEM	Franchised Distributors/ Aftermarket	Stocking/ Broker/ Independent	Unknown Sources	Open Market Surplus Recyclers

Applying Anti-Counterfeit Controls Across DOD Acquisition Process



Abbreviation:
APB – Acquisition Program Baseline
DFAR – Defense Federal Acquisition Regulations
EMD – Engineering Manufacturing Development
FOC – Full Operational Capability
FRP – Full Rate Production
GIDEP – Government Industry Data Exchange Program
IOC – Initial Operational Capability
LRIP – Low Rate Initial Production
MS – Milestone
OCM – Original Component Manufacturer
OEM – Original Equipment Manufacturer

FY12 National Defense Authorization Act (NDAA)

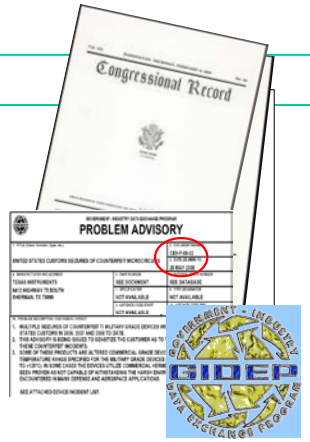
Focus—Detection and Avoidance of Counterfeit Electronic Parts

Tenets:

- Directs DOD to ***assess current anti-counterfeiting practices*** and implement "risk-based" policies to address counterfeit
- Requires DOD and contractors whenever possible to buy electronic parts from the Original Component Manufacturer (OCM) or its authorized distributor(s)
- Directs DOD to ***establish a "Trusted Supplier" program*** to certify organizations that comply with industry standards on anti-counterfeiting
- Institutes cost recovery for counterfeit items
- ***Re-affirms mandatory reporting (GIDEP) for incidents internal and external to DOD***
- Requires the Secretary of Homeland Security to establish a methodology for the enhanced inspection of electronic parts after consulting with the Secretary of Defense as to the sources of counterfeit parts in the defense supply chain

Specific Actions:

- ***Establish DOD-wide definition***
- ***Issue anti-counterfeit mitigation guidance***
- ***Issue remedial action guidance***
- ***Create reporting process (GIDEP)***
- ***Develop process to analyze and act on reports***
- ***Incorporate in DFAR anti-counterfeit language***



SASC Report

Counterfeit Electronic Parts in DOD Supply Chain

- China is dominant source for counterfeit electronic parts in DOD defense systems
- Suspect counterfeit parts on critical defense systems (C-27J, C-130J, AH-64, P-8A etc.) not reported in a timely fashion into GIDEP
- Counterfeit parts drive up costs in DOD operations and sustainment
- Defense industry's reliance on unvetted distributors for parts used in critical military applications
- Defense industry's weakness in test and inspection of electronic parts create opportunities for counterfeiters to exploit
- DOD and industry failed to report counterfeit parts through GIDEP

Memorandum from Acting USD/AT&L Overarching Anti Counterfeit Guidance

- Addresses an area of critical concern while Department policy is in coordination
- Provides definition
- Emphasizes
  - Risk-based approach
  - Leverages Program Protection Plan and non-conforming processes
  - Directs use of existing contracting clauses and data elements to ensure traceability and reporting on critical items for contractors and subcontractors
  - Use of anti-counterfeiting standards
  - Disposal of counterfeit items
  - Training

The Honorable Frank Kendall
Acting Under Secretary of Defense for AT&L

Current and Potential Activities

Department-wide

- ***Drafting definition--an item that is an unauthorized copy or substitute that has been identified, marked, and/or altered by a source other than the item's legally authorized source and has been misrepresented to be an authorized item of the legally authorized source."***
- ***Drafting policy***—addresses Commerce and GAO findings and recommendations, and NDAA requirements
  - *Calls for establishing preventive measures to mitigate counterfeit risks*
  - *Requires inventory controls and testing*
  - *Requires personnel training*
  - *Requires collaboration with industry and law enforce (utilizing best practices)*
  - *Establishes centralizing reporting using GIDEP*
- ***Developing counterfeit awareness training courses***
- Implemented counterfeit detection course for student technicians at DOD microelectronics school @ NSWC, Crane Indiana
- Collaborating with Defense Associations (NDIA, AIA & SAE) and Law Enforcement (DCIS, FBI, Customs, Border Patrol, etc)

Defense Logistics Agency

- ***Performing full range of physical testing on sample electronic components*** at DLA Land & Maritime in Columbus, OH
- Buying electronic circuit items in stock classes 5961 & 5962 using ***qualified supplier distributor lists*** (QSLD)
- ***Requiring critical electronic component suppliers to submit pre-award traceability documents for materiel***
- Purchasing critical systems (space, nuclear, flight sys, etc) items from only ***approved sources with 100% inspection***
- ***Requiring new electronic suppliers to provide certificate of conformance*** and performing visual and physical checks

Military Services

- ***Establishing Counterfeit Programs for electronics***:
  - *Navy—limited electronic component testing @ Navy Electronics Depot, Crane Indiana*
  - *Army—limited electronic component testing @ Army Depot Tobyhanna, Pennsylvania*
  - *Air Force—limited inspection/diagnostics electronic component testing @ Air Logistics Centers*
- Performing sample visual checks of incoming material at maintenance depots and supply centers
- Performing ***supplier facility and process audits for critical weapon system (space, nuclear, flight sys, etc) components***
- Posting counterfeit alerts, bulletins, and advisories in supply and repair centers
- Assisting law enforcement and Justice Dept with criminal case prosecution

Microelectronics Counterfeit Inspection

- Risk-based inspection of non-OCM, mission essential parts and critical safety items is necessary

- Inspection and test processes include:
  - Optical microscopes to catch obviously deficient parts (blacktopped, scratched, erroneous codes, etc)
  - X-Ray Inspection and Fluorescence Radiation to check for bonding inconsistency, damage, and physical impurities
  - 5000x Scanning Electron Microscope(SEM) Inspection to examine surface for grain disturbance due to modification (e.g. sand blasting)
- Outcome is verification part performs according to all required specifications
- Adopt industry standards for counterfeit inspections

Identification and Disposition

Inventory control

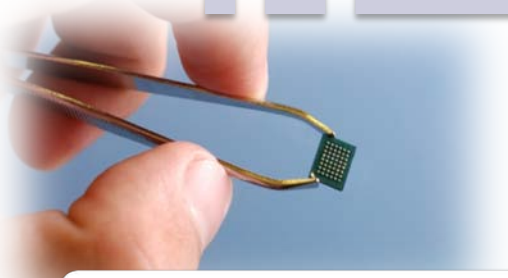
- Materiel control and traceability program
- Quality management systems
- Systemic test and verification processes

Reporting/Information Sharing

- Use product quality deficiency reporting processes
- Conduct engineering analysis and authenticity determination
- Report in GIDEP

Disposition

- Hold for law enforcement disposition
- Dispose according to federal logistics information system code guidance
- Execute suspension and debarment process as required



DoD Policy standardizing processes across supply chain

Reporting and Information Sharing

- GIDEP is official repository connecting Government, Industry, Law Enforcement (internal and external) for counterfeit data

- Weapon System Managers and FMS program offices responsible for sharing counterfeit information with affected customer countries

- International Traffic in Arms Regulations (ITAR) exemption required for partner country GIDEP access

Moving Forward

- ✓ Formalize risk-based approach using Program Protection Plan and System Engineering Plan methodology
- ✓ Improve processes and developing policy for counterfeit prevention and detection
- ✓ Strengthen and standardize existing identification and disposition processes, standards, and contract requirements for counterfeit materiel across industry/DoD supply chain
- ✓ Leverage GIDEP as centralized reporting tool for counterfeit incidents and information sharing
- ✓ Review how to streamline information sharing with allied/coalition countries

BACK UP

Potential Standards

	Published	Under-Development	Used For Electronic Parts	Used For Procurement Processes & Control	Used For Test and Inspections	Used for Quality Management/ Assurance	Anti-Counterfeit Specifics
AS 5553	X		X	X	X		X
AS 6081		X	X	X		X	X
ARP 6178	X		X	X	X		X
AS 6174		X	X	X	X	X	X
AS 6171		X	X		X		X
ARD 6884		X	X				X
AS 9120/A	X		X			X	
AS 9100	X		X			X	
ISO 9001	X			X		X	
JESD 31	X		X	X		X	

AS 5553 - Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition
AS 6081 - Counterfeit Electronics Parts; Avoidance Protocol, Distributors
ARP 6178 - Fraudulent/Counterfeit Parts; Tool for Risk Assessment of Distributors
AS 6174 - Counterfeit Materiel; Detection, Mitigation, and Disposition
AS 6171 - Test Methods Standards; Counterfeit Electronic Parts
ARD 6884 - Terms and Definition – Fraudulent/Counterfeit Electronic Parts
AS 9120/A - Quality Management System: Requirements for Aviations, Space and Defense Distributors
AS 9100 - Quality Systems – Aerospace – Model for QA in Design, Development, Production, Installation and Servicing
ISO 9011 - Quality Management Standard
JESD 31 - General Requirements For Distributor of Commercial and Military Semiconductor Devices